

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-127969

(43)Date of publication of application : 25.05.1993

(51)Int.Cl.

G06F 12/00
G06F 12/14

(21)Application number : 03-289757

(71)Applicant : HITACHI LTD

HITACHI SEIBU SOFTWARE KK

(22)Date of filing : 06.11.1991

(72)Inventor : FUJIOKA NORIHIKO

TAKAHASHI NORIYUKI

NISHIMURA HIROKO

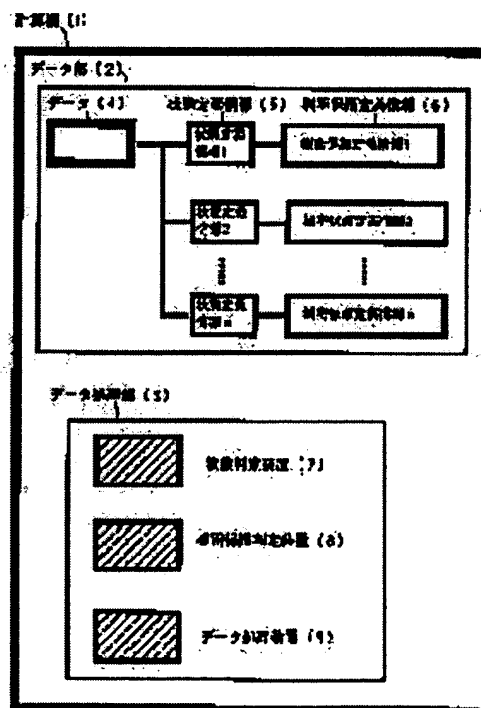
KUSHIRO YASUO

(54) SECRET INFORMATION PROTECTING METHOD

(57)Abstract:

PURPOSE: To execute different secret protection in accordance with the state of data by referring to the state definition information of the data stored before hand together with the data at the time of accessing to the data and discriminating the state of the data concerned.

CONSTITUTION: A computer 1 includes a data storage part 2 and a data processing part 3, and the data storage part 2 includes the data 4. The data processing part 3 is constituted to a state discriminating device 7, a secret protection discriminating device 8, and a data processor 9. Here, the data 4 taken out of the data storage part 2 is sent to the state discriminating device 7, and the state of the data 4 is discriminated. Besides, the data 4 is sent to the secret protection discriminating device 8, and the secret protection is executed in conformity with secret protection information in the state of the data 4, and at the time when access is to be suppressed, the transfer of the data 4 to the data processor 9 is suppressed. Besides, in the case that the access to the data 4 is permitted, the data 4 is sent to the data processor 9.



THIS PAGE BLANK (USPTO)

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-127969

(43)公開日 平成 5 年(1993) 5 月25日

(51)Int.Cl.⁵

G 0 6 F 12/00
12/14

識別記号

5 3 7 A
3 2 0 A

庁内整理番号

7832-5B
9293-5B

F I

技術表示箇所

審査請求 未請求 請求項の数 3 (全 13 頁)

(21)出願番号 特願平3-289757

(22)出願日 平成 3 年(1991)11月 6 日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(71)出願人 000233365

日立西部ソフトウェア株式会社

大阪府大阪市中央区北浜 3 丁目 5 番29号

(72)発明者 藤岡 典彦

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72)発明者 高橋 典幸

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74)代理人 弁理士 小川 勝男

最終頁に続く

(54)【発明の名称】 機密情報保護方法

(57)【要約】

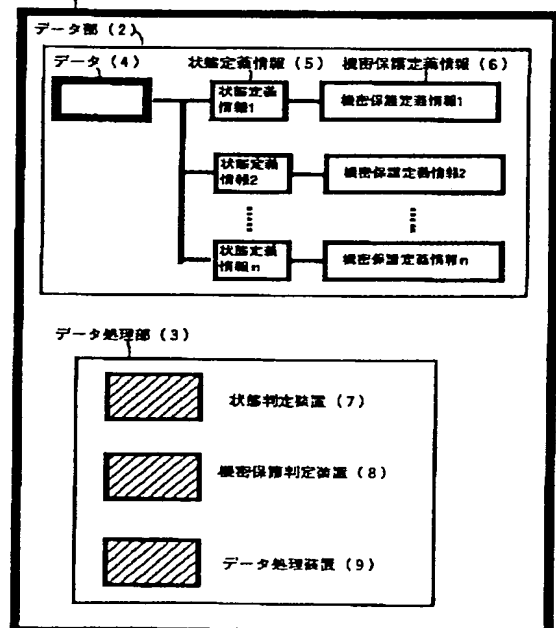
【目的】 データの状態の変化に従って異なる機密保護を施すことを可能にする。

【構成】 計算機 1 はデータ 4 を含むデータ格納部 2 と状態判定装置 7 と機密保護判定装置 8 とデータ処理装置 9 を含むデータ処理部 3 を含む。

【効果】 データの状態の変化に従って異なる機密保護を施すことが可能になる。

計算機 (1)

図 1



1

【特許請求の範囲】

【請求項 1】 データの読みだしと更新及び削除を制限する機構を備えるデータ格納部及びデータ処理部を持つ計算機システムにおいて、状況に応じて変化するデータに対して、あらかじめ、データの状態の変化を定義する状態定義情報を一緒に格納しておき、該データから該状態定義情報を取り出して参照し、該状態定義情報からデータの状態の遷移を判定し、該状態に対応する固有の機密保護情報を割り当てることを特徴とする機密情報保護方法。

【請求項 2】 請求項 1 記載の機密情報保護方法においてあらかじめ、複数のデータを包含する集合データの状態の変化を定義する状態定義情報を一緒に格納しておき、該集合データから状態定義情報をとりだして参照し、該状態定義情報から集合データの状態を判定し、該状態に対応する固有に機密保護情報を割り当てることを特徴とする機密情報保護方法。

【請求項 3】 請求項 1 記載の機密情報保護方法において時刻を監視する手段を設け、該手段から得られる時系列情報と状態定義情報を照合し、データの状態の遷移を判定する手段を持つことを特徴とする機密情報保護方法。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 計算機システムにおいてデータの読みだしと更新、及び削除を制限する機密保護の方式に関する

【0002】

【従来の技術】 従来、データに対する機密保護を行う技術には例えば、特開昭 62-248048 号公報 ファイルの機密保護方式で示されるように複数のユーザからアクセス可能な共用のデータに対して読みだしと更新、及び削除を制限する手段としてデータに固有の機密保護情報を対応づけておく。機密保護情報には、読みだしと更新、及び削除を許可する権限コードが格納されており、データにアクセスする際にユーザに割り当てた権限コードと照合して、その結果に従って処理を行うか否かを判定して不当なデータアクセスを抑止していた。

【0003】

【課題を解決するための手段】 本発明の目的はデータの読みだしと更新及び削除を制限する機構を備えるデータ格納部及びデータ処理部を持つ計算機システムにおいて、状況に応じて変化するデータに対して、あらかじめ、データの状態の変化を定義する状態定義情報を一緒に格納しておき、保護を行おうとするデータから状態定義情報をとりだして参照し、該状態定義情報からデータの状態を判定し、該状態に固有に対応する機密保護情報を割り当てることで達成することができる。

【0004】

【作用】 データにアクセスする際にあらかじめデータと

2

共に格納されたデータの状態定義情報を参照して当該データの状態を判定する。認識したデータの状態に対応した機密保護情報を参照して機密保護のための情報を取得してデータに対する不当な操作を抑止する。

【0005】 さらに複数のデータを含む集合データにも単体のデータと同様の処理を実現する。さらに時刻の変化にともなってデータの状態を制御する機構を付加してデータの状態の遷移を自動的におこなう。

【0006】

【実施例】 本発明の実施例を図面を用いて詳細に説明する。

【0007】 図 1 に本発明の基本的な構成を示す。計算機 1 はデータ格納部 2 とデータ処理部 3 を含む。データ格納部 2 はデータ 4 を含む。データ処理部 3 は状態判定装置 7 と機密保護判定装置 8 とデータ処理装置 9 から構成される。処理 1-1 においてデータ格納部 2 から取り出されたデータ 4 は状態判定装置 7 に送られる。状態判定装置 7 ではデータの状態を判定する。処理 1-2 においてデータは機密保護判定装置 8 に送られる。機密保護判定装置 8 おいてデータの当該状態における機密保護情報に従って機密保護を行い、アクセスを抑止するべき時には処理 1-4 においてデータをデータ処理装置 9 へ送ることを抑止する。また当該データへのアクセスを許可する場合には処理 1-4 によりデータをデータ処理装置 9 へ送る。

【0008】 図 2 はデータ 4 の構成を示す。データ 4 はデータ本体部 4-1 と状態定義情報 5 と機密保護定義情報 6 から構成される。

【0009】 状態定義情報 5 は当該データが取りえる状態の数の定義があり、機密保護定義情報 6 は、状態定義情報 5 に対応づけられている。

【0010】 図 3 はデータ 4 の詳細を示す。データ 4 はデータ本体 4-1 と状態指示子 4-2 と状態定義情報 5 へのポインタを含む。状態指示子 4-2 はデータの状態を示すものでありデータの状態の変化にともなってその値を変化させる。状態定義情報 5 は、データがとることができる状態を示す状態定義値 5-1 と他の状態定義情報 5 へのポインタ 5-2 と当該状態時に対応する機密保護定義情報 6 へのポインタ 5-3 を含む。機密保護定義情報 6 はデータ本体 4-1 に対する読みだしと更新および削除の操作の許可または禁止の情報を含む。

【0011】 データ 4 をデータ処理部 3 で処理を行うとき状態判定装置 7 において状態指示子 4-2 を参照して、当該状態の状態定義情報 5 を選択してさらに当該状態に対応する機密保護定義情報 6 を選択する。次に機密保護判定装置において選択した機密保護定義情報 6 に基づいてデータ本体 4-1 に対する読みだしと更新及び削除の権限のチェックを行い、その結果それぞれの操作が許可されているときにはデータ処理装置 9 においてデータ本体 4-1 の操作を行う。

3

【0012】図4はデータ処理部3の処理の流れを示す。

【0013】データ4に対して読みだし・更新・削除の処理を行うとき、まず状態判定装置7でポインタ4-3をたどって状態定義情報5を選択する(処理111)。

【0014】次に状態指示子4-2と状態定義値5-1を比較して(処理112)2つの値が一致すれば処理114へ処理を進める。2つの値が異なればポインタ5-2をたどって、次の状態定義情報5を選択して(処理113)さらに処理112を繰り返す。次に機密保護判定装置8でポインタ5-3をたどって当該状態時に対応する機密保護定義情報6を選択する(処理114)。

【0015】次に当該処理が許可されているか否かを判定して(処理115)、当該処理が禁止されていれば操作不可のエラー処理を行い(処理117)、当該処理が許可されている場合にはデータ処理装置9においてデータ処理を実行する(処理118)。

【0016】図5は図3に複数のデータ4を包含する集合データを定義する集合データ定義情報12を追加したものである。集合データ定義情報12には、集合データ名称12-1と状態指示子12-2とポインタ12-3と集合データが含むデータ4を示すポインタ12-4を含む。集合データ定義情報12に対しても機密保護情報を割り当てて、単体のデータと同様の処理により集合データの機密保護を行うことができる。

【0017】図6は、図1の構成に時刻監視装置11を追加した構成図である。

【0018】状態判定装置7において状態を判定する時に、時刻による状態定義情報と時刻を照合して当該時刻におけるデータの状態を判定することが出来る。

【0019】図7は、図3のデータ部に状態制御情報を追加したデータ構造を示す。

【0020】状態制御情報10には状態変更時刻10-1とポインタ10-2を含む。状態変更時刻10-2は、当該データ4が状態を遷移する時刻を格納しておき、ポインタ10-2から遷移する状態の定義を示す。状態制御情報10はデータ4の中のポインタ4-4から示される。

【0021】図8に図4の処理に時刻による状態の制御を行う処理を示す。

【0022】状態判定装置7でデータ4の状態を判定する前に処理211においてポインタ4-4をたどって状態制御情報10を選択して処理212において状態変更時刻10-1と現在の時刻を比較する。現在の時刻が状態変更時刻10-1と等しいか過ぎているとき状態指示子4-2を更新する(処理213)。

【0023】図9は、図1の構成において、状態判定装置7と機密保護判定装置8をデータ格納部2に移した構成である。データの機密保護をデータ格納部で行うことによりデータ処理部の処理負荷を軽減できる。

4

【0024】図10、図11は本発明の具体的な実施例を示す図である。

【0025】図11は資料の置かれる変化に対応するその変化固有の機密保護マトリックスを示す。

【0026】例えば、作成者Aにおける資料の作成中という状態には図11の①が対応し、読み書きが可能であるが、審査する人Bの資料の作成中という状態の場合には図11の④が対応するため、読み書きはできない。

【0027】また、資料の保存という状態では総合管理者Eに対して図11の②が対応するため、総合管理者Eだけが資料を読むことのみが可能となり、他のA～Dには図11の④が対応するため、その資料には読むことも書くこともできない。

【0028】この図で示されるように資料の置かれる状態(データの変化)と権限を持つ人毎に対応する機密マトリックスが決まっているため、状態にあわせた機密保護が可能になる。

【0029】

【発明の効果】本発明によりデータ状態遷移に従った機密保護を行える。また、単体のデータだけでなく、集合データについてもデータの状態遷移に応じた機密保護を行うことができる。さらに時刻の変化に基づくデータの状態遷移に応じた機密保護を行うことができる。

【図面の簡単な説明】

【図1】本発明の基本的な構成を示す図、

【図2】状態定義情報と機密保護定義情報を示す図、

【図3】状態定義情報と機密保護定義情報の詳細を示す図、

【図4】データ処理部の処理の流れを示すフローチャート、

【図5】集合データ情報を示す図、

【図6】本発明の構成に時刻監視装置を追加した構成を示す図、

【図7】データ部に状態制御情報を追加したデータ構造を示す図、

【図8】時刻による状態の制御を行う処理の流れを示すフローチャート、

【図9】状態判定装置と機密保護判定装置をデータ格納部に移した構成を示す図、

【図10】本発明による具体的な実施例を示す図、

【図11】機密保護マトリックスを示す図。

【符号の説明】

- 1…計算機
- 2…データ格納部
- 3…データ処理部
- 4…データ
- 5…状態定義情報
- 6…機密保護定義情報
- 7…状態判定装置
- 8…機密保護判定装置

5

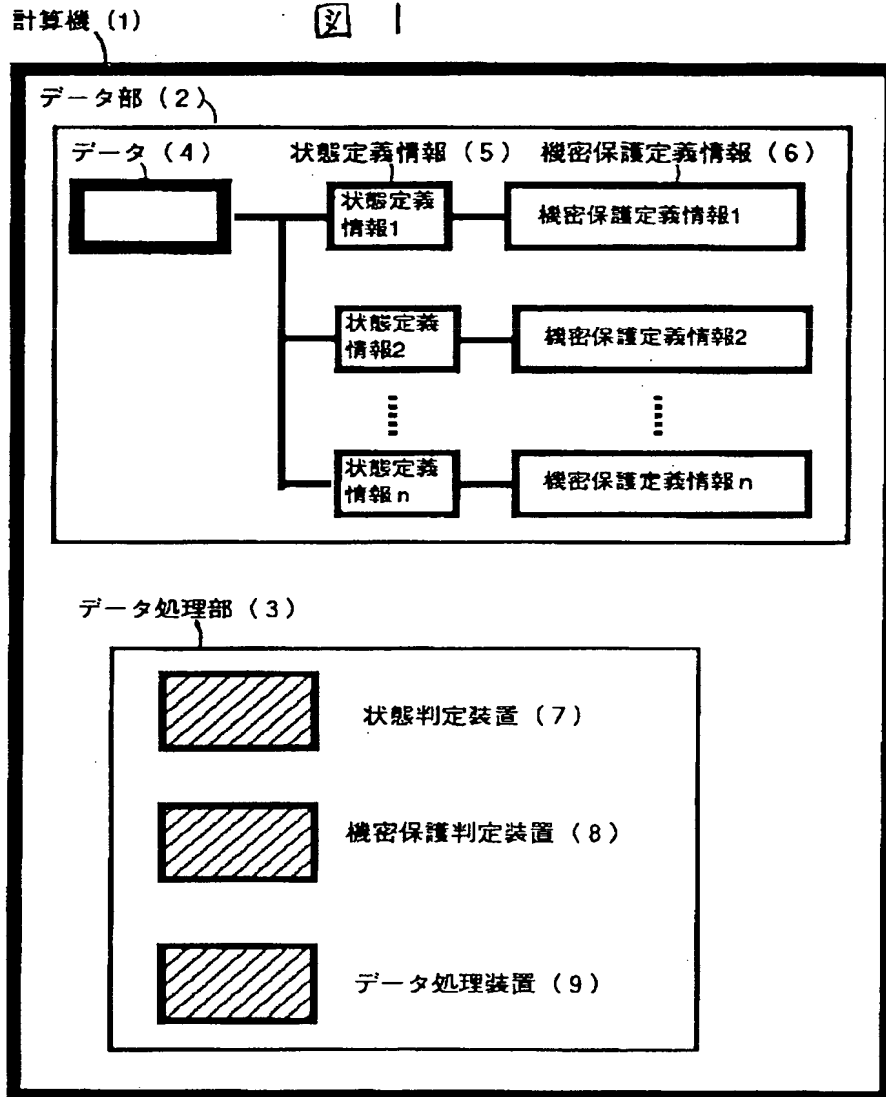
9...データ処理装置
10...状態制御情報

* 11...時刻監視装置

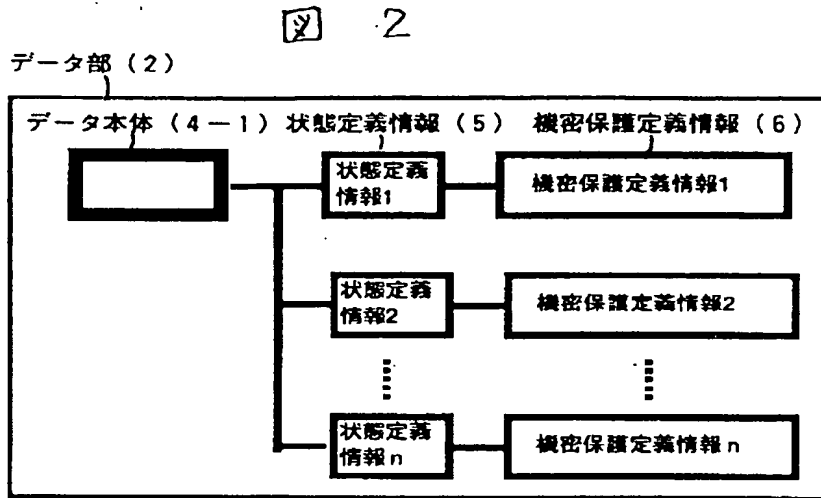
* 12...集合データ定義情報

6

【図1】

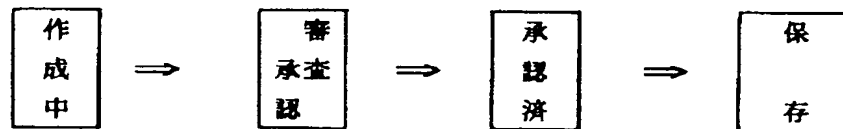


【図 2】



【図 10】

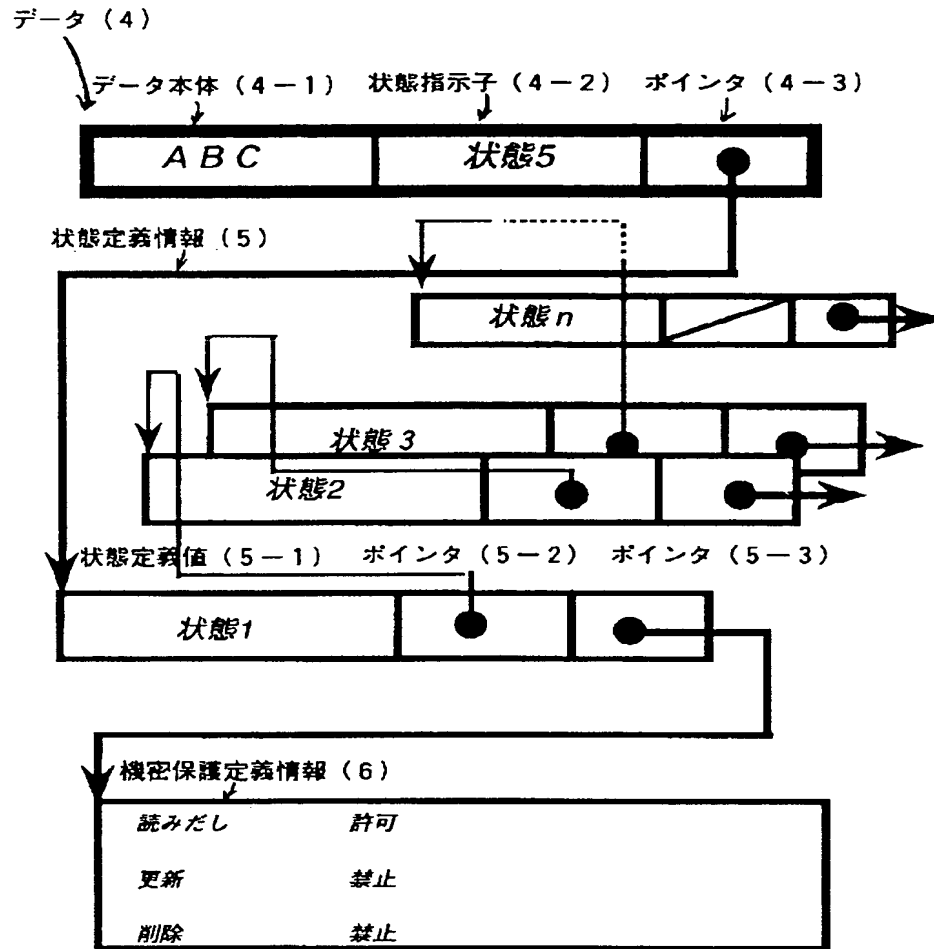
図 10



	READ	WRITE	READ	WRITE	READ	WRITE	READ	WRITE
作成者 A	○	○	○	×	○	×	×	×
一般の人 B	×	×	×	×	○	×	×	×
審査する人 C	×	×	○	○	○	×	×	×
承認する人 D	×	×	○	○	○	×	×	×
総合管理者 E	○	×	○	×	○	×	○	×

【図 3】

図 3



【図4】

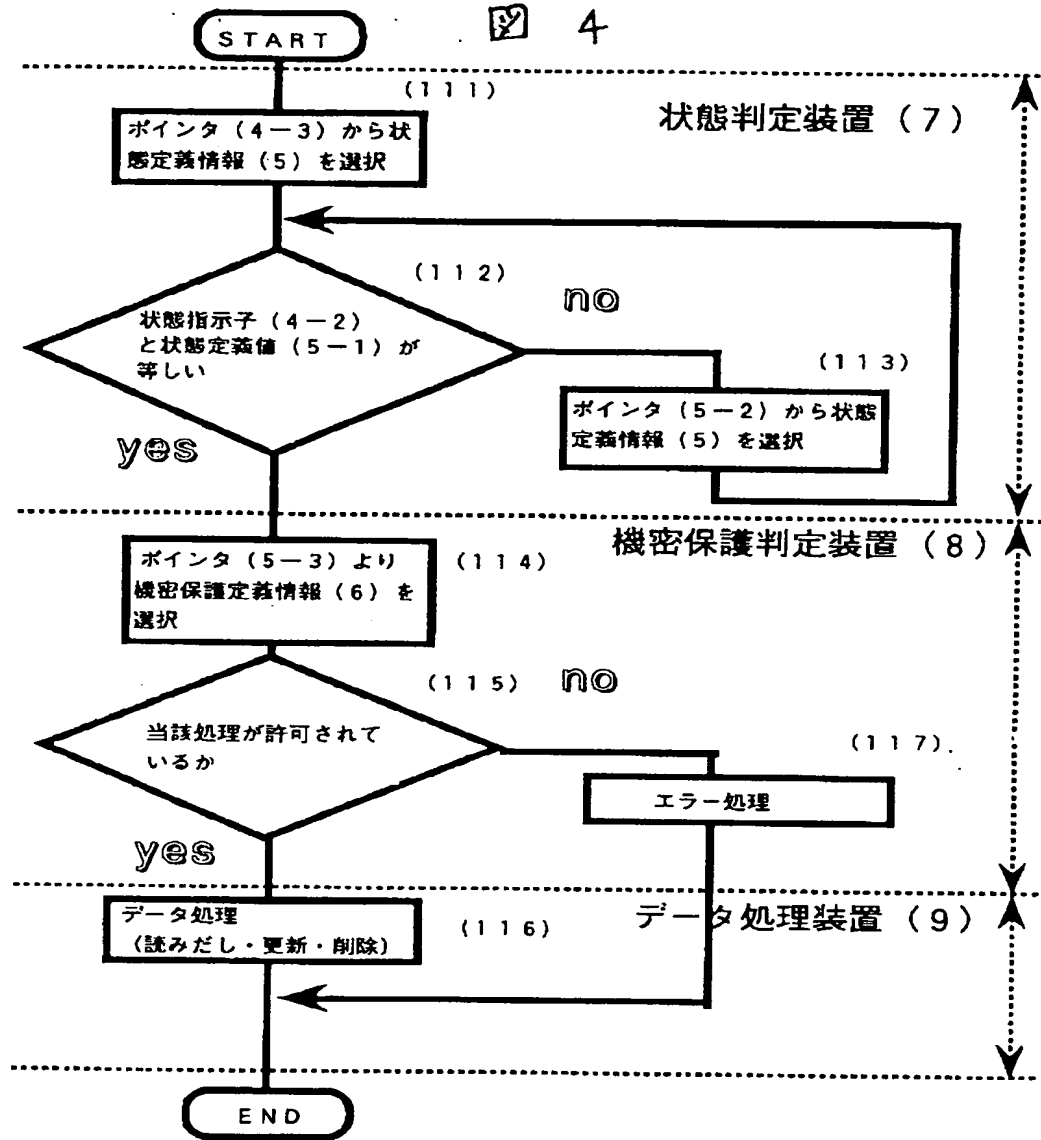
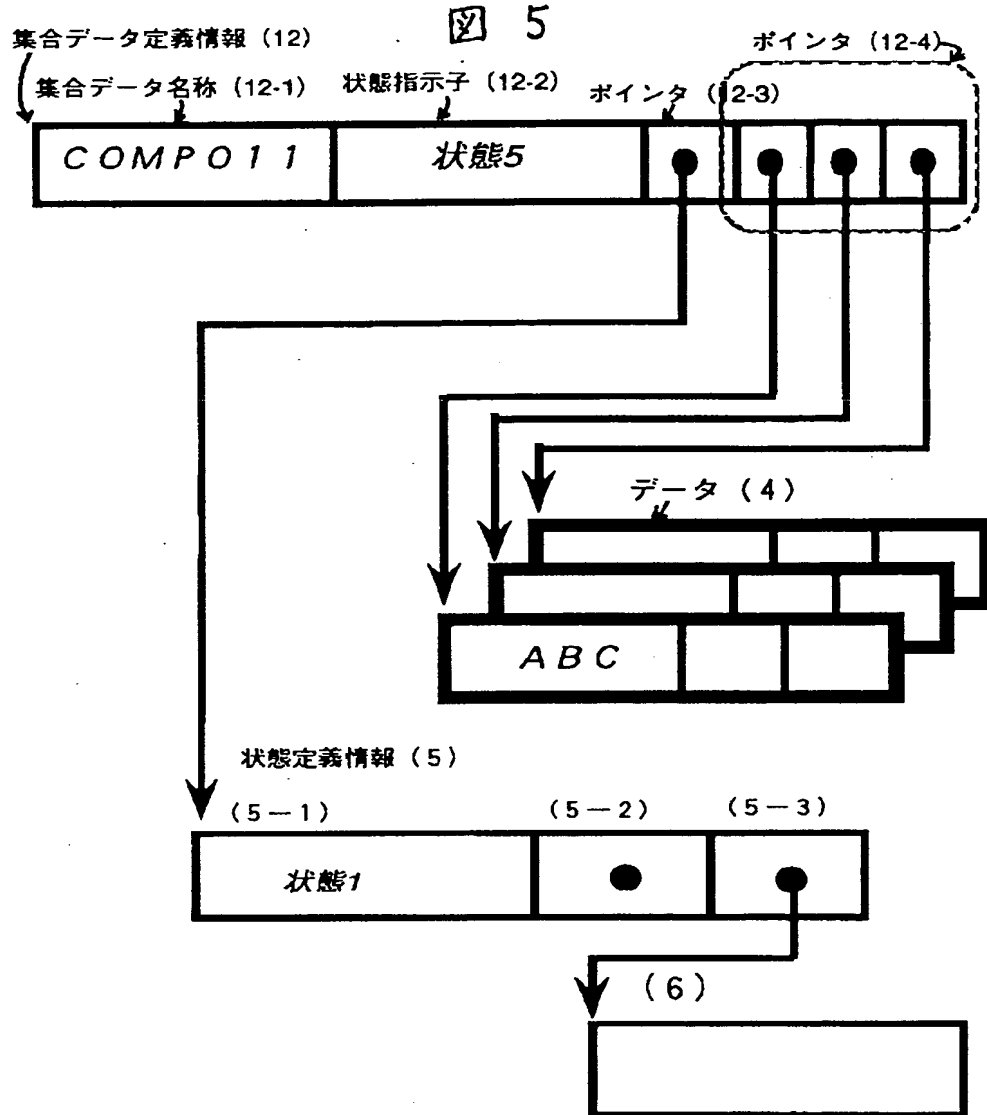
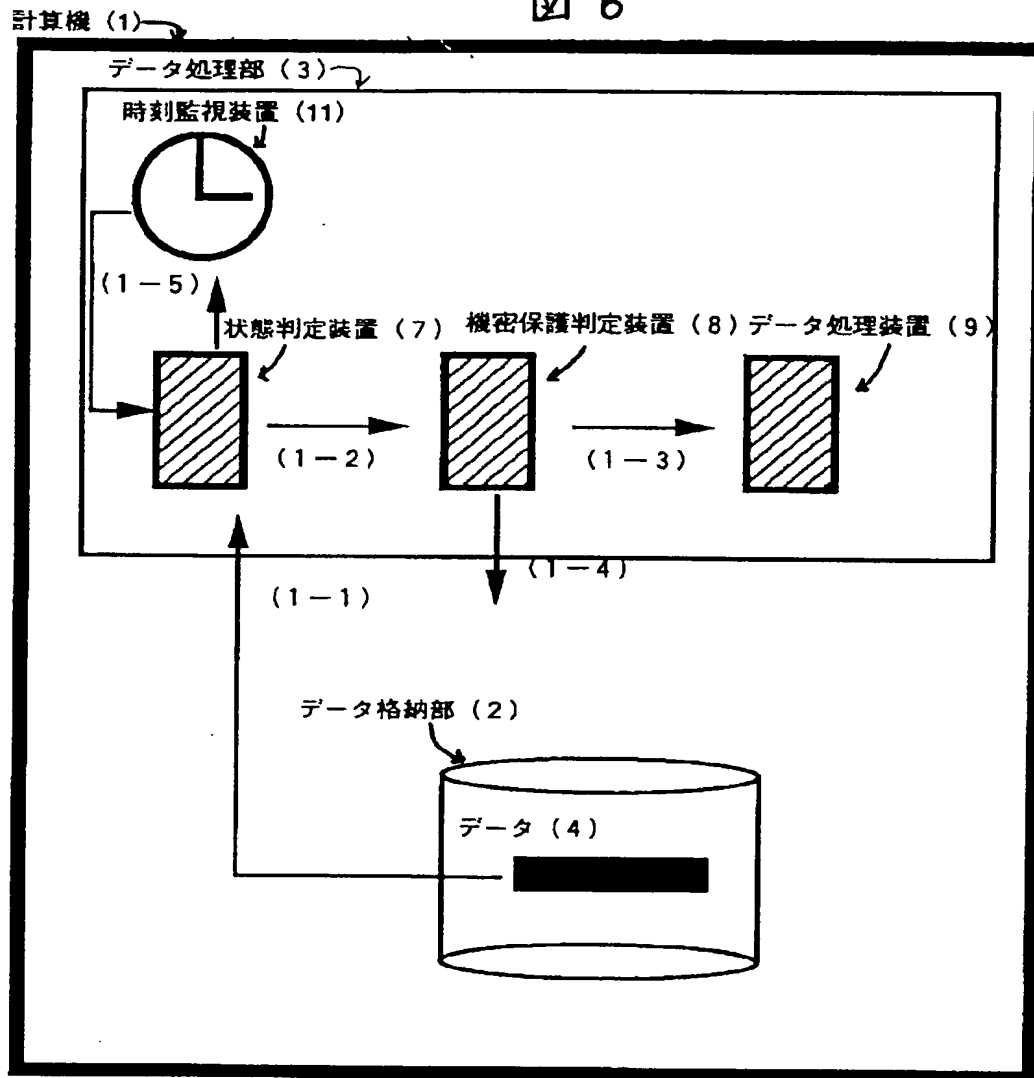


图 5

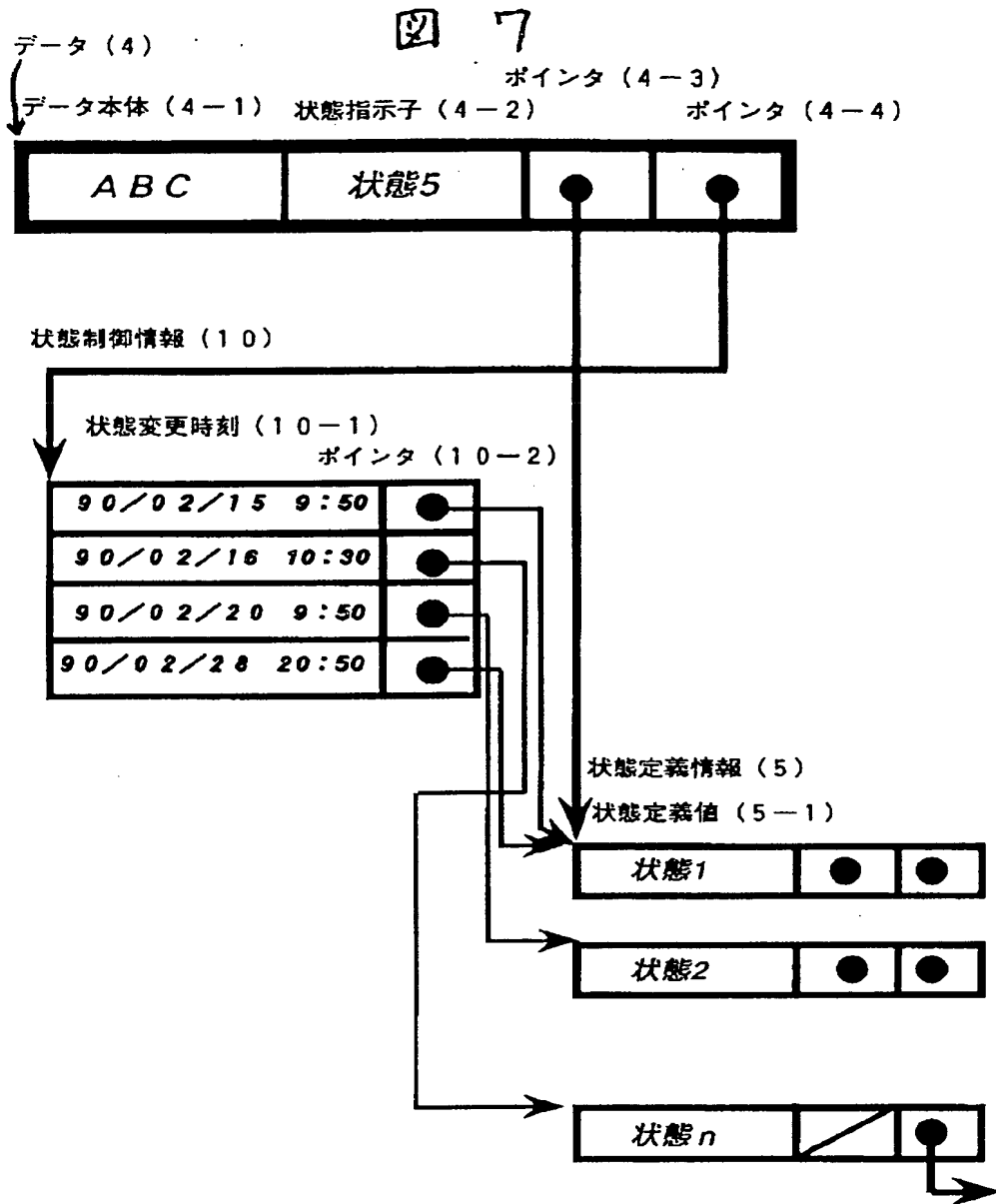


【図 6】

図 6

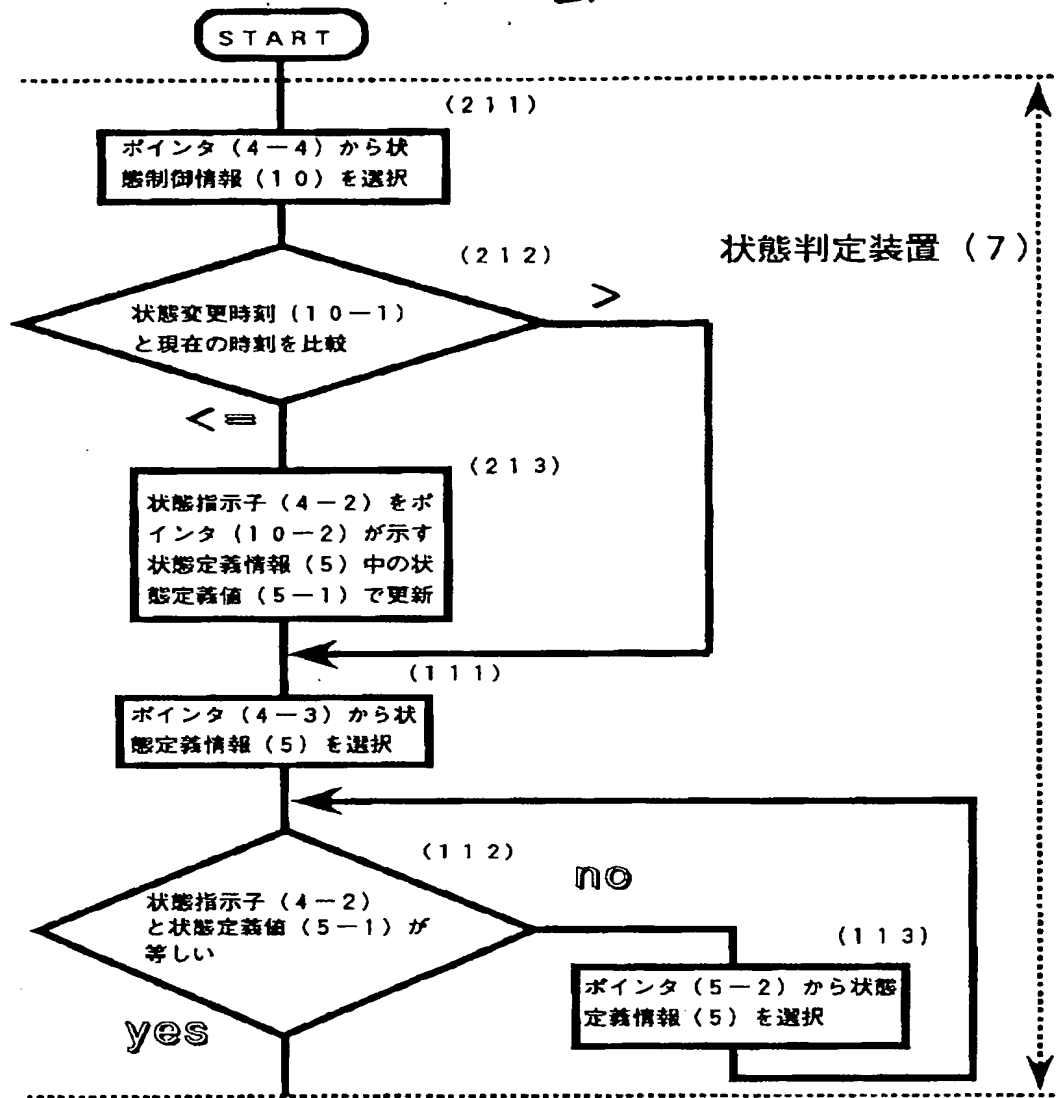


【図 7】



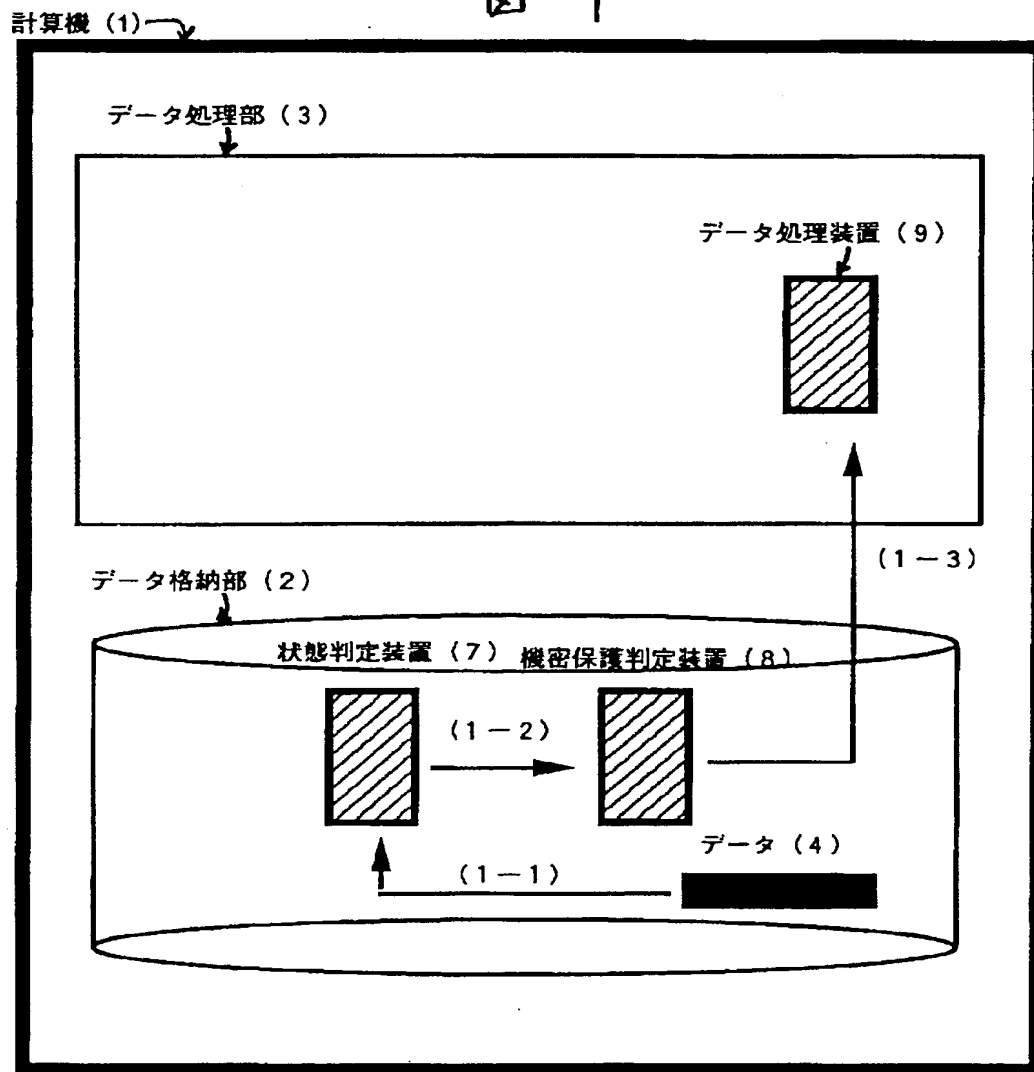
【図 8】

図 8



【図 9】

図 9



【図11】

図11

機密保護マトリックス

	READ	WRITE
①	○	○
②	○	×
③	×	○
④	×	×

フロントページの続き

(72)発明者 西村 弘子
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア開発本部内

(72)発明者 久代 康雄
大阪府大阪市中央区北浜三丁目5番29号
日立西部ソフトウェア株式会社内

THIS PAGE BLANK (USPTO)